ENTERPRISE EMAIL

ARMY SERVICE ACQUISITION

REPORT TO CONGRESS
(as required by Section 353 of the National Defense Authorization Act for Fiscal Year 2012)

Headquarters, Department of the Army
February 2012

Preparation of this report cost the Department of Defense
a total of approximately $187,000 in Fiscal Year 2012.
Generated on 2012 Feb 01 1420

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Section 353 of the National Defense Authorization Act for Fiscal Year 2012 directed the Secretary of the Army to designate efforts to consolidate email into an Enterprise Email Service as a formal acquisition program. It also restricted obligation and expenditure of fiscal year 2012 funds until 30 days after receipt of this report.

The relevant provisions of the law are as follows:

> **SEC. 353. DESIGNATION AND LIMITATION ON OBLIGATION AND EXPENDITURE OF FUNDS FOR THE MIGRATION OF ARMY ENTERPRISE EMAIL SERVICES.**
>
> (a) DESIGNATION.—The Secretary of the Army shall designate the effort to consolidate its enterprise email services a formal acquisition program with the Army acquisition executive as the milestone decision authority. The Secretary of the Army may not delegate the authority under this subsection.
>
> (b) LIMITATION.—None of the funds authorized to be appropriated by this Act or otherwise made available to the Department of Defense for fiscal year 2012 for procurement or operation and maintenance for the migration to enterprise email services by the Department of the Army may be obligated or expended until the date that is 30 days after the date on which the Secretary of the Army submits to the congressional defense committees a report on the acquisition strategy for the acquisition program designated under subsection (a), including certification that existing and planned efforts for the program comply with all existing regulations pertaining to competition. The report shall include each of the following:
>
> > (1) A description of the formal acquisition oversight body established.
> >
> > (2) An assessment by the acquisition oversight body of the sufficiency and completeness of the current validated requirements and analysis of alternatives.
> >
> > (3) In any instances where the validated requirements or analysis of alternatives has been determined to be insufficient, a plan for remediation.
> >
> > (4) An assessment by the Army Audit Agency to determine the cost savings and cost avoidance expected from each of the alternatives to be considered.
> >
> > (5) An assessment of the technical challenges to implementing the selected approach, including a security assessment.
> >
> > (6) A certification by the Secretary of the Army that the selected approach for moving forward is in the best technical and financial interests of the Army and provides for the maximum amount of competition possible in accordance with section 2302(3)(D) of Title 10, United States Code.
> >
> > (7) A detailed accounting of the funding expended by the program as of the date of the enactment of this Act, as well as an estimate of the funding needed to complete the selected approach.

This report responds to each requirement of law stated above. The Army halted migration to Enterprise Email when the NDAA was enacted. From March to December of 2011, the Army migrated 302,361 users to Enterprise Email. Those users, including a number of our most senior officials and four-star commanders, use Enterprise Email as their primary messaging and calendar/scheduling service in the performance of their missions. The majority of these users enjoy better service that is more secure and costs less than the service provided by legacy Army systems, as evidenced by user survey results, a security assessment and direct communications among senior leaders.

Additionally, the Army is in the process of capturing these procedures and processes for application on future enterprise services and infrastructure projects. This oversight will ensure that all strategic considerations, including competition and contract impacts, are included in the business planning process. We are currently employing this method for Enterprise Collaboration Services.

Enterprise Email is the Army's #1 information technology efficiency initiative. The Under Secretary of the Army originally included its planning for Enterprise Email in the Army Business Transformation Plan submitted to the Congress on October 1, 2010. This was updated in the March 1, 2011 Department of the Army 2011 Annual Report on Business Transformation, Providing Readiness at Best Value, found at URL: http://armyobt.army.mil/downloads/2011-annual-report-on-business-transformation.pdf**.** The Army issued, in December 2010, an Execution Order to all commands to migrate to Enterprise Email. In addition, the Secretary of Defense included Army information technology efficiencies from consolidation of email servers and data centers in his January 2011 report on efficiency initiatives.

The Army is the first military department to adopt the Department of Defense's Enterprise Email service as its single provider of email. A cost-benefit analysis, conducted in 2009-2010 and published in 2011, analyzed four alternatives and determined that acquiring Enterprise Email as a service from the Defense Information Systems Agency (DISA) was the best approach for the Army's generating force (tactical email systems are not being replaced by Enterprise Email).

The following summarizes the response to each of the concerns contained in Section 353 of the National Defense Authorization Act. Details on each are contained either in the main body of the report or in attachments.

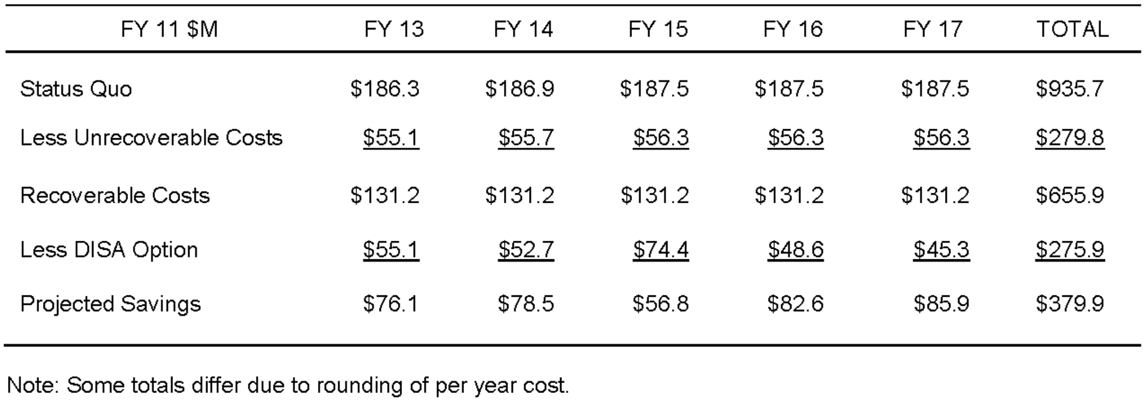
(1) The Army will use two bodies to support all enterprise services decisions. The Army Systems Acquisition Review Council (ASARC), chaired by the Army Acquisition Executive (AAE), is the formal acquisition oversight body for Enterprise Email service acquisition. The Business Systems Information Technology (BSIT) Executive Steering Group, chaired by the Under Secretary of the Army/Chief Management Officer (USA/CMO), will validate requirements and the associated analysis of alternatives. A description of the oversight concept as it applies to Enterprise Email is included in section 1. Additionally, the Army will establish a similar process for future enterprise services and infrastructure projects.

(2) On January 18, 2012, the Business Systems Information Technology 3-Star Working Group, chaired by the Deputy Chief Management Officer, unanimously

concluded that the cost-benefit analysis for Enterprise Email was sufficient for making an acquisition decision, and unanimously confirmed the requirements document. On January 20, 2012, the ASARC assessed and deemed sufficient both the validated requirements and the analysis of alternatives included in the cost-benefit analysis. The ASARC was informed by extensive discussion of the assumptions, criteria-weighting and overall analysis contained within the cost-benefit analysis report. The Army Acquisition Executive designated the Enterprise Email service as a formal acquisition program in an Acquisition Decision Memorandum dated January 25, 2012, which can be found in attachment 1 to this report.

(3) While not necessary now, should the requirements or analysis of alternatives need to be updated or are otherwise determined insufficient at any future point, the USA/CMO, will direct appropriate remediation action.

(4) The Army Audit Agency (AAA) completed its assessment of the estimated costs of each of the alternatives in the cost-benefit analysis and published its report on January 19, 2012. Results of AAA's review are contained in attachment 2 to this report. AAA found no material issues with the four alternatives presented, but determined that the projected cost savings did not include all necessary factors. As a result, AAA concluded the savings claimed (originally more than $100 million per year), though still significant, were overstated. AAA's adjusted estimates of costs for the status quo and the selected alternative, and projected savings starting in FY13, are summarized below:



FY 11 $M	FY 13	FY 14	FY 15	FY 16	FY 17	TOTAL
Status Quo	$186.3	$186.9	$187.5	$187.5	$187.5	$935.7
Less Unrecoverable Costs	$55.1	$55.7	$56.3	$56.3	$56.3	$279.8
Recoverable Costs	$131.2	$131.2	$131.2	$131.2	$131.2	$655.9
Less DISA Option	$55.1	$52.7	$74.4	$48.6	$45.3	$275.9
Projected Savings	$76.1	$78.5	$56.8	$82.6	$85.9	$379.9

Note: Some totals differ due to rounding of per year cost.

(5) Mitigation of all technical challenges to Enterprise Email implementation is complete; how these issues were overcome is described in the main body of this report. Regarding security: over the summer/fall of 2011, the National Security Agency (NSA) and the Defense Information Systems Agency (DISA) conducted a comprehensive security review of Enterprise Email. The effort began with a focused, multi-week review of the Enterprise Email architecture by the NSA Architecture Group and the DISA Security Architecture Analysis Team/Penetration Testing (SAAT/PT) team, and concluded with an onsite assessment by an NSA Blue Team in combination with DISA's SAAT/PT team and DISA Certification Support personnel. While the review did identify implementation-level issues and procedural items that must be addressed, it found no

general architectural issues and highlighted several key security advantages of Enterprise Email over the status quo.

(6) Based upon 1 through 5 above, the selected approach for Enterprise Email is in the best technical and financial interests of the Army. Enterprise Email provides for the maximum amount of competition possible in accordance with 10 USC § 2302(3)(D). Of the $525 million expended to date by DISA to establish the enterprise infrastructure at the Enterprise Service Centers, which are supporting the enterprise email service, 88% has been via full and open competition, 6.5% placed on small business 8a set-aside contracts, and 2% executed using brand name competitions. A synopsis of the contracts DISA is using is contained in attachment 3 to this report. The Army Acquisition Executive issued a second Acquisition Decision Memorandum (ADM) on February 3, 2012 that provided additional direction to the newly established Army Enterprise Email program; a copy is at attachment 4 to this report.

(7) As of December 31, 2011, the date of enactment of the National Defense Authorization Act, the Army had expended $71.7M on Enterprise Email ($62.7M to DISA and $9.0M for Army responsibilities including migration). To complete the selected approach, the estimated funding requirement is $12.7 million, including full migration by March 31, 2013, and operation of a formal program office. Sustainment through September 30, 2012 will cost $42.0M. A detailed accounting is included in section 7 of the main report.

Conclusion

Upon delivery of this report, all actions required by Section 353 of the NDAA are complete, including designation of the effort as a formal acquisition program with the Army Acquisition Executive as the milestone decision authority.

In accordance with statutory authority for inter-agency acquisitions, Enterprise Email is an acquisition of services between DoD components and will not strictly adhere to the requirements of Department of Defense Instruction (DoDI) 5000.02. For contracted services with commercial vendors, DoDI 5000.02, Enclosure 9, “Acquisition of Services” guidance will be followed. Accordingly, program documentation will be tailored to address unique program requirements.

Overall, the Department of Defense Enterprise Email solution enhances centralization and eliminates disparate systems, which, in turn, supports the Army’s Business Transformation Plan. It will improve the Army’s security posture, enable standardization of hardware and software, improve configuration control, and centralize administration and support while enhancing financial transparency. The cost-benefit analysis – which was independently validated by the Deputy Assistant Secretary of the Army for Cost and Economics, with estimated costs of the alternatives subsequently reviewed by the Army Audit Agency – supports DISA-provided Enterprise Email as the best option among four alternatives (status quo, managed service provided by a commercial vendor, Army Knowledge Online and managed service provided by DISA). The commercial and DISA options best met the validated requirement; of these two, the DISA option is the least costly for the Army to implement.

The Army's utilization of Enterprise Email is accomplished through an annual Service Level Agreement (SLA) between the Army and DISA, and represents a sound business decision with quantifiable and non-quantifiable benefits to the Army. The Army realizes significant cost savings by leveraging existing Army enterprise license agreements, competitively awarded DISA contracts, and existing DoD and Army networks. The annual nature of the SLA provides the opportunity to periodically review the Enterprise Email selected option and consider alternative service providers.

Way Ahead

The Enterprise Email migration process is managed through normal operational channels, with joint military orders issued weekly to synchronize all activities. The decision to migrate is made by Army commanders when their conditions are right to ensure success with no impact to operations. Planning is ongoing with the intent of restarting migration 30 days after this report is provided to Congress. Proven capacity exists to migrate up to 7,000 users per business day. The objective is to reach full operational capability by September 30, 2012, and to complete all migrations by March 31, 2013.

The Army Audit Agency will begin an audit of Enterprise Email performance and cost savings in February 2012.

BACKGROUND

Today the Army spends a disproportionate amount of resources managing and securing its current, segmented email systems. The simple act of determining the amount of money spent on email Army-wide can be difficult due to disparate implementation and intertwining with other IT services.

Between 1995 and 2007, Army networks developed in a decentralized fashion (centralized policy by design with decentralized execution). Installations were responsible for determining the best method to deliver capabilities to their tenant organizations, and each major organization determined the best method to provide coherent, integrated solutions to its subordinate components, often spread across the globe.

A variety of efforts to consolidate services and networks over time achieved varying levels of success, but none provided the holistic solution the Army needed. For example, in the late 1990s, Army Knowledge Online (AKO) was established. It was initially an experimental project of the General Officer Management Office and later became a portal to provide web-based email, central authentication capabilities and remote content storage for Army users worldwide. Although AKO offered email capabilities, the lack of adequate functionality and lack of integration with local networks and network operations hindered its widespread adoption as the Army's single email service provider during this timeframe.

In 2008, the Army determined that it still had at least 18 different network enclaves in existence with redundant Microsoft Exchange Email systems across the globe. The large number of disparate and redundant networks, along with the high number of servers and personnel required to maintain them over the life cycle of the systems, resulted in high costs and significant operational inefficiencies across the Army. Most Army installations hosted their own Microsoft Exchange servers and employed the necessary support staff. Moreover, AKO also hosts an email service used by the entire Army, resulting in a second, duplicate mailbox for approximately 800,000 Army users and presenting an unnecessary, duplicative cost to the Army.

This segmentation of service produced a number of inefficiencies and operational risks for the Army, such as:

1. Lack of calendar-sharing across organizations
2. Lack of delegation privileges to users in other organizations
3. Inefficiencies as Soldiers and Civilians transfer between duty stations
4. Duplicate email services deployed throughout the Army
5. Duplicate email administration responsibilities
6. Underutilized hardware

7. Potential security vulnerabilities due to multiple disparate authentication mechanisms, including in some cases, username/password
8. Lack of Continuity of Operations (COOP) capability
9. Non-compliance with statutory and regulatory requirements to journal specific email messages

In November 2007, the Gartner Group provided the Army Chief Information Officer/G-6 a report stating that the Army should consolidate its segmented Exchange resources into a single collaborative system.

In 2008, the Department of Defense started exploring the idea of creating a single DoD-wide email solution. A tiger team of subject matter experts from every Service, the Joint Staff, NSA and other DoD agencies was assembled to identify DoD enterprise requirements and determine which product should be used to provide a consolidated email solution for DoD. As a result of their detailed analysis, in September 2008, the DoD team recommended that Microsoft Exchange Server be used for the DoD-wide consolidated email solution. Studies performed by Gartner and MITRE supported the team's favorable scalability and feasibility findings, as well as the team's assessments of potential cost savings and operational benefits from a more capable, global, collaborative service.

DISA began developing an implementation plan and provided monthly updates to the DoD Enterprise Guidance Board (EGB), which is chaired by the Deputy DoD Chief Information Officer and includes representation from each Service's Chief Information Officer (CIO) and the Joint Staff. Additionally, a DISA-led joint information assurance and security team leveraged the email tiger team's work to make recommendations on enhancing the security of the email system and improving the authentication methodology so that any user could authenticate (log in securely) to Enterprise Email from any DoD network with approved DoD smart cards, such as the Common Access Card (CAC). In February 2009, DoD approached Microsoft leadership with this issue, which required changes to its Exchange server and Outlook client software in order to provide the enhanced authentication and security capabilities. Microsoft made these changes at no cost to DoD and now includes these changes as a part of its mainstream commercial releases.

In March 2009, upon realization that the DoD Enterprise Email program had not progressed significantly, the Army became concerned that it would not be able to use the program to meet its own modernization and consolidation needs. The Army submitted a proposal to the EGB, asking to take the lead for Enterprise Email, with the stated intent of leveraging commercial capabilities by releasing a request for proposals (RFP) to industry. The Army used the DoD requirements document as the basis for the RFP, refining it significantly according to market research and analysis by reducing scope and eliminating unnecessary requirements. The release of a draft RFP in March 2010 resulted in significant industry response that seemed to demand an even further reduction in basic requirements. The Army conducted a cost-benefit analysis comparing the status quo, AKO and a commercial option. The commercial option, while not the least costly, best met the requirements.

As the RFP process took significantly longer than anticipated and the extended timeline for execution would not have allowed the use of FY10 funding, the Army determined it was best not to release the formal RFP before reexamining internal DoD options for email capabilities.

In June 2010, at the request of the Army CIO/G-6, DISA submitted to the Army a proposal to provide enterprise email capabilities from its nine Defense Enterprise Computing Centers spread across the globe, using the recently released 2010 version of Microsoft Exchange. (The Common Access Card authentication security enhancements were in beta testing and not yet available, but their release was imminent.) The Army provided DISA both the DoD Enterprise Email requirements document and the down-scoped/altered Army EE RFP requirements so that an implementation plan could be developed and costs refined.

In August-September 2010, the Army conducted a lengthy cost-benefit analysis of the DISA option, specifically comparing DISA's proposal against the commercial option, appropriately adjusted to Army vice DOD-scale requirements to assure an apples to apples comparison. During this phase of analysis, the status quo and AKO options were not reconsidered, having been ranked lower in the earlier phase. The commercial and DISA options were both good fits for the Army's requirement, with the DISA option considerably less costly. The Army committed $53.9 million to DISA to begin the project in September 2010.

The table on page 11 provides a high-level summary comparing the costs and benefits of the four alternatives as presented to Army leadership in 2010, with updated savings predictions from the January 19, 2012 Army Audit Agency report.

In the end, the commercial and DISA options best met the requirement, with DISA being the least costly.

In late October 2010, the disparate email requirements documents were merged together into a single set of formal requirements, which were delivered to DISA on November 2, 2010. In December 2010, DISA stood up the first beta capability for Army functional testing. Issues were identified, and Microsoft and DISA made the requisite software and configuration updates. Regression testing showed that all significant problems were addressed by early February 2011.

Cost vs Benefit Comparison				
Course of Action	**Full Cost (FY11-17)**	**Savings (FY13-17) (AAA)**	**Quantifiable Benefits**	**Non-Quantifiable Benefits**
COA 1 – Status Quo	$1,308M	N/A		• No migration (i.e., disruption) to users
COA 2 – Commercial MSP	$ 516.1M	$328.5M	• Reduces cost of email service • Increases storage per mailbox	• Reduces IT footprint • Centralized funding and architecture decisions • Consistent policies and processes • Meets CAC authentication requirements • Conforms to Army Data Center Consolidation Plan (ADCCP) objectives • Better vendor support • Consistent security posture across geographies • Additional email tools for end users
COA 3 – AKO	$237.9M	$493.5M	• Reduces cost of email service • Increases storage per mailbox	• Reduces IT footprint • Centralized funding and architecture decisions • Consistent policies and processes
COA 4 – DISA as the MSP	$466.4M	$379.9M	• Reduces cost of email service • Increases storage per mailbox	• Reduces IT footprint • Centralized funding and architecture decisions • Consistent policies and processes • Meets CAC authentication requirement • Conforms to ADCCP objectives • Better vendor support • Consistent security posture across geographies • Additional email tools for end users • Meets Blackberry/SME PED requirement • Fully integrated with all mission assurance security infrastructure, monitoring and Cyber Defense operations • Enhanced collaboration across organizations

In late December 2010, the Army released an Execution Order notifying all elements both to begin preparations for the transition to Enterprise Email and to participate in the development of a migration schedule that would complete Army migration by December 31, 2011. Army Cyber Command had to grant some extensions on the migration schedule, however, because several commands encountered an operating system compatibility issue. The smart card authentication security solution in Enterprise Email requires, for Windows-based computers, the Windows Vista or Windows 7 operating system. Several commands had specific technical reasons for continuing to use Windows XP for a limited time period. These commands developed and submitted plans of actions with milestones for their migration to either Vista or Windows 7 (and then to Enterprise Email), and were given deadline extensions in accordance with their program dates. As of the date of this report, the latest migration extension granted is March 31, 2013.

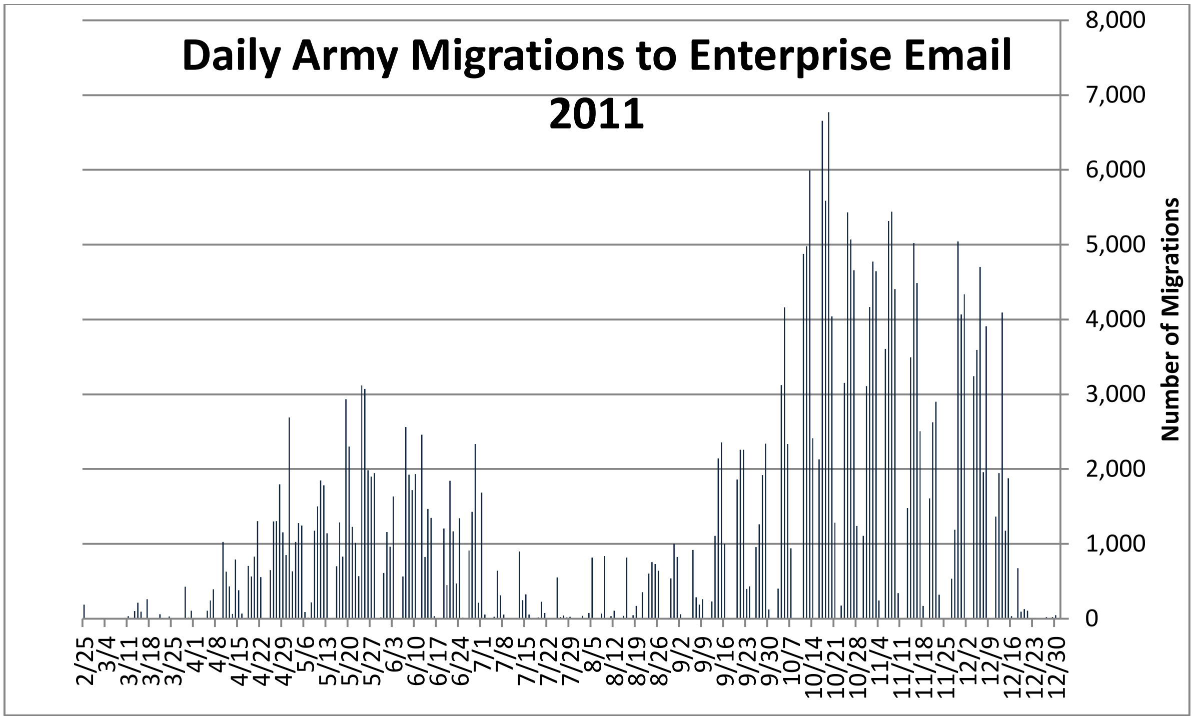
The Army CIO/G-6 and Network Enterprise Technology Command (NETCOM) conducted full-scale operational tests of Enterprise Email by migrating themselves to the system and using it exclusively during February and March 2011. Once satisfied with the new service's capabilities, the Army began migrating installations and commands from their legacy Exchange systems to Enterprise Email. The Director, DISA and the Army CIO/G-6 signed the Enterprise Email Service Level Agreement on August 1, 2011, with the agreement that it would be updated in February 2013 and reviewed annually thereafter.

The Army is responsible for migrating its users to the DISA-provided service. Migrations are executed from regional migration centers operated by NETCOM Theater Signal Commands/Brigades using an Army-developed migration tool from Communications-Electronics Command's Software Engineering Center. Fly-away support teams provide pre-migration assistance on each post/camp/installation.

As the system began to experience loads beyond the first few thousand users, the Army and DISA identified specific systemic issues that needed analysis and resolution. The Commanding General, NETCOM, who leads the migration effort on behalf of the Army, paused new migrations in June 2011, as both the Army and DISA needed time to address the technical issues and refine and rehearse business practices designed to ensure smooth migration and quality user support post-migration. Processes were improved and technical configuration changes were implemented to resolve systemic network and load-balancing issues. The Army and DISA captured lessons learned and developed tactics, techniques and procedures to resolve issues and provide standardized solutions.

The conditions necessary to lift the pause were met in late August 2011, and migration resumed in early September 2011, with 302,361 migrations completed through December 2011.

By November 2011, migration capacity reached 7,000 mailboxes per business day. The limiting factor was coordination with and availability of the impacted users/organizations so that current operations were not affected. The figure below shows the number of daily migrations performed during calendar year 2011:



The balance of this report provides more detailed information for each of the requirements set forth in Section 353.

1. SERVICE ACQUISITION FORMAL OVERSIGHT

Section 353 requires that the Army describe the formal acquisition oversight body established to obtain Enterprise Email services as a formal acquisition program with the Army Acquisition Executive (AAE) as the Milestone Decision Authority.

The Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA (ALT)) exercises overall supervision of acquisition, technology and logistics matters of the Department of the Army, pursuant to 10 USC § 3016. As mandated by 10 USC § 2330 and in accordance with AR 70-13, *Management and Oversight of Service Acquisitions*, the ASA(ALT), as the AAE, has overarching responsibility for the Army's management and oversight of the acquisition of service contracts. The Army Systems Acquisition Review Council (ASARC), chaired by the AAE, has initiated the formal Enterprise Email program and is providing oversight of the Army's acquisition of enterprise services and infrastructure within the Army's Enterprise Infrastructure Environment.

The AAE, advised by members of the ASARC and after review of the information provided to that body, has determined the most appropriate method to procure Enterprise Services, to include Enterprise Email. The acquisition strategy for Enterprise Services, in this case Enterprise Email, balances the need for competition with other key considerations. Acquisition oversight of Enterprise Services utilizes key performance measures to assess overall program progress.

The Army will conduct acquisition program reviews at critical points in the Enterprise Email program's life cycle. These reviews will serve as a forum to surface and resolve significant issues affecting program execution and to recommend appropriate action to the AAE.

The decision review process will support program stability. Accordingly, significant program funding and requirements changes will not be introduced without assessing and considering their impact on the overall acquisition strategy and established program baseline. Affordability will be a key consideration. The AAE retains the authority to direct the program to evaluate alternative solutions.

During management oversight reviews, the AAE will ensure that the views of all stakeholders are presented and considered in evaluating the service provider's performance. The AAE will receive accurate and timely program documentation and information to enable firm decisions and the issuance of clear direction.

The ASARC membership is as follows: Assistant Secretary of the Army (Acquisition, Logistics and Technology) (Chair), the Vice Chief of Staff of the Army, the Assistant Secretary of the Army (Financial Management & Comptroller), the Assistant Secretary of the Army (Installations, Energy & Environment), the Assistant Secretary of the Army (Manpower & Reserve Affairs), the Chief Information Officer/G-6, the Deputy Chiefs of

Staff G-1, G-2, G-3/5/7, G-4 and G-8, the Deputy Under Secretary of the Army Test and Evaluation Executive, the General Counsel, the Director, Office of Small Business Programs, and the Commanding Generals of Army Materiel Command and Training and Doctrine Command.

As stated in the acquisition decision memorandum of January 25, 2012 (attachment 1) it is important to note that, in accordance with statutory authority for interagency acquisitions, the acquisition of Enterprise Email services is being accomplished between DoD components and will not strictly adhere to the requirements of DoD Instruction (DoDI) 5000.02. For contracted services with commercial vendors, the Army follows DoDI 5000.02, Enclosure 9, “Acquisition of Services”. Accordingly, program documentation is tailored to address unique program requirements.

2. REQUIREMENTS AND ANALYSIS OF ALTERNATIVES

Section 353 requires the Army’s Enterprise Email acquisition oversight body to conduct an assessment of the sufficiency and completeness of the validated requirements and analysis of alternatives.

The Army’s acquisition process consists of a series of Army-level management reviews and decisions. The process begins with a Materiel Development Decision (MDD). At the MDD, the Milestone Decision Authority (in this case, the AAE in conjunction with the ASARC) authorizes the program’s entry into the acquisition management system at a point where phase-specific entrance criteria and statutory requirements can be accommodated. The reviews are structured in logical phases.

On January 18, 2012, the Business Systems Information Technology (BSIT) 3-Star Working Group, on behalf of the BSIT Executive Steering Group, met to review the status of complying with section 353 of NDAA 2012. This included confirmation of the Enterprise Messaging as a Managed Service (EMMS) requirements and the analysis of alternatives included in the Army’s June 8, 2008 Enterprise Email service cost-benefit analysis (CBA). The group discussed extensively the assumptions, weighting, and overall analysis contained within the CBA, and the Army Audit Agency also reported its assessment of the CBA. The BSIT unanimously concluded that the CBA was sufficient for making a decision and was ready for presentation to the Army Systems Acquisition Review Council (ASARC). The BSIT also unanimously validated the Army EMMS requirements.

The AAE convened the ASARC on January 20, 2012, for the purpose of making the Materiel Development Decision for Enterprise Email. The ASARC reviewed the requirements for Army messaging (as described in the approved EMMS requirements specification), the range of materiel solution approaches that could address the Army’s identified capabilities gaps, affordability constraints, the current status of the Army’s

Enterprise Email initiative and the recommended phase of entrance into the acquisition life cycle.

As a result of the ASARC review, the AAE determined that the validated requirements and analysis of alternatives were sufficient to move forward with the creation of Enterprise Email as a formal acquisition program and granted the program a Materiel Development Decision. Program Executive Office, Enterprise Information Systems was directed to establish a project office for acquisition of services to support Army Enterprise Email (attachment 1). The AAE issued a second Acquisition Decision Memorandum on February 3, 2012 to provide additional direction to the newly established Army Enterprise Email program, and to direct that the program will enter the acquisition life cycle post Initial Operating Capability (attachment 4). Implicit in these decisions is the finding that of the alternatives presented, the selected approach with DISA represented the best value to the Army.

3. REMEDIATION PLAN FOR REQUIREMENTS AND ANALYSIS OF ALTERNATIVES (IF NECESSARY)

Section 353 requires that, once the Army establishes a formal acquisition oversight body for Enterprise Email, that body will assess the requirements and analysis of alternatives. Based on this assessment, a remediation plan will be established as necessary.

As noted above, both the BSIT and the ASARC determined that the requirements document and the analysis of alternatives contained in the cost-benefit analysis for Enterprise Email were sufficient. However, our examination of the Enterprise Email procurement revealed the need to develop a formal procurement process suitable not only for addressing any future issues with Enterprise Email but also for acquiring other enterprise services or infrastructure initiatives. The following procedures are applicable to future instances of services procurement.

The BSIT serves as the oversight body for reviewing requirements and the analysis of alternatives for other enterprise services or infrastructure initiatives. The ASARC is the oversight body for acquisition program execution. If presented with a negative report from the BSIT, the Under Secretary of the Army, in his capacity as Chief Management Officer, will direct appropriate remediation action (potential actions might include a requirements review with top cost drivers identified, or consideration of new alternatives that might improve cost-effectiveness or minimize disruption to Army personnel). The remediation will be coordinated by the Army's Office of Business Transformation (OBT) with any affected Headquarters, Department of the Army staff elements and the secretariat. (For Enterprise Email, this includes the AAE and its assigned Program Executive Officer, the Chief Information Officer/G-6, the G-3 and the G-8.) Based on degree of sufficiency, remediation will occur in multiple parts, and action will take one or multiple forms. OBT will fully coordinate with each office to ensure that the following processes are accomplished as required.

a. Part One: Requirements and Analysis

- The functional proponent establishes service requirements, conducts an analysis of alternatives and presents findings to the BSIT for approval. (For Enterprise Email, the functional proponent is the Army CIO/G-6.)
- The BSIT validates service requirements and the analysis of alternatives, or, through the USA/CMO, directs revision of requirements and analysis of other constraints or sourcing alternatives that must be considered within the context of a revised analysis of alternatives.
- The functional proponent (supported by the AAE, the appropriate Program Executive Office and OBT) revises requirements, conducts a revised analysis of alternatives and presents each to the BSIT for approval by the USA/CMO.
- Once the revised requirements and analysis are approved, the AAE and the functional proponent will present the revised plan to the USA/CMO for final approval and implementation direction.

b. Part Two: Execution of Acquisition Process

- The AAE or duly designated Program Executive Office develops a plan of action and milestones.
- The G-8 adjusts program funding, as required.
- The Program Executive Office, working with applicable supporting organizations, implements the plan.
- The Program Executive Office provides, as established by the ASARC, periodic status reports throughout remediation implementation, and the ASARC provides monthly reports to the USA/CMO.

4. ARMY AUDIT AGENCY ASSESSMENT

Section 353 requires an assessment by the Army Audit Agency to determine the cost savings and cost avoidance expected from each of the alternatives to be considered. AAA’s report is provided in its entirety without additional comment at attachment 2.

5. ASSESSMENT OF TECHNICAL CHALLENGES

Section 353 requires an assessment of the technical challenges to implementing the selected approach, including a security assessment.

INTRODUCTION

A variety of technical challenges exist in implementing the selected approach. Some are from a functional or operational perspective; others include the ability to secure and defend the system from cyber attack. While solutions for the most significant technical concerns have been implemented, the Army recognizes that security is an ongoing challenge. As the capabilities of the adversary increase, so must our ability to protect, detect and react to various threats and vulnerabilities.

This section of the report is organized into two parts. The first outlines the more significant technical challenges associated with enterprise-level email and describes actions taken to address those elements. The second part examines security-related challenges, leveraging the (positive) results of a recent security assessment performed jointly by the National Security Agency (NSA) and DISA's Security Architecture Analysis Team/Penetration Testing (SAAT/PT) team.

PART 1 – TECHNICAL CHALLENGES

The technical challenges the Army identified – identity management, dual persona, cross-boundary/two-fact authentication, workstation baseline updates, bandwidth, migration tools, and local national/foreign military/volunteer users – have been addressed in a number of ways, as described below.

Identity Management

As a global DoD service, Enterprise Email required development of an identity management solution containing unique identities for every DoD user (contractor, civilian, active duty and reserve component service members). This was further complicated by the fact that many individuals in DoD have more than one relationship with the Department, such as being a civil servant and a reservist at the same time. For some time, DoD has used the Electronic Data Interchange Personal Identifier as the unique identifier for every person issued a Common Access Card (CAC). While this 10-digit number identifies a specific person, it does not differentiate the different roles (or "personas") a person may hold, such as a contractor also serving as a member of the Army Reserve.

DoD was already implementing an enterprise identity structure with unique, but related, identities for each persona an individual might have. Working with all of the components and the Defense Manpower Data Center (DMDC) – the authoritative data warehouse for everyone who has a present (or past) relationship with DoD – DISA developed the DoD “Enterprise User Name, Display Name and E-mail Address Standard” to address the enterprise identity and multiple persona issues. The naming standard provides a new email naming convention that is tied to the enterprise identity but is unique for every persona and is sustainable for more than 250 years (based on analysis performed by DMDC). In addition to user identities, the naming standard also addresses enterprise identities for “non-person entities” (NPEs), such as conference rooms, organizational mailboxes and distribution lists.

The solution for using this enterprise identity in Enterprise Email required near-real-time synchronization of data from the DMDC database, as well as management of email-specific attributes, such as entitlements for mailboxes, mobile devices, archiving and quota limits, and data retention. Additionally, DMDC and DISA had to develop data feeds that would allow automated transfer of authoritative data so that DISA’s entire database of accounts is based on official authoritative information from DMDC. DISA, in conjunction with the Army, developed the Identity Synchronization Service (IdSS) to solve these myriad challenges. IdSS is an automated solution that maintains data consistency between DMDC and Enterprise Email, provides management capabilities to provision mailboxes programmatically, and automatically decommissions accounts as users separate from DoD.

It should be noted that IdSS is a common DoD enterprise service provided by DISA and is intended to support many enterprise applications, with the DoD’s Enterprise Email service being the first use.

Dual Persona

Although the naming standard addressed the policy details of how to solve enterprise identity for individuals who have more than one persona, the technical solution for how each persona would uniquely authenticate using a particular CAC had to be developed. DoD established a joint working group in 2009, with all of the Services and DISA, to examine the pros and cons of several possible courses of action. The working group arrived at a solution that would cause the least impact to non-dual-persona users, utilize existing Public Key Infrastructure (PKI) certificates, and still provide distinct cryptographic login credentials for each persona. The chosen solution for unclassified email, using the Personal Identity Verification (PIV) standard established in response to Homeland Security Presidential Directive - 12, was tested and validated before moving forward. The PIV interoperability standard extends the DoD Electronic Data Interchange Personal Identifier to identify both the person and his or her role. Dual persona users have two CACs, each with a unique PIV identifier specific to the persona. The procedures and methodology for authentication using the federal PIV certificate were coordinated with the DMDC and DISA before implementation.

Cross-Boundary/Two-Factor Authentication

One key aspect of the enterprise system is the ability for each person to authenticate with two-factor credentials. This DoD requirement represents significantly stronger security than username/password. Historically, two-factor login and email access using the standard DoD CAC were authenticated through the user's home station Microsoft Active Directory (AD) forest. However, Enterprise Email is a "cross-forest/cross-boundary" solution, meaning a user's network account and privileges reside in an AD forest at each user's home station but his email account information and Exchange service provider reside within a separate Enterprise Service-dedicated, limited-functionality AD forest. Thus, a user must authenticate through his home station AD for generic network access, but subsequently authenticate across AD boundaries for email access.

This isolation of email-related attributes provides a number of security benefits. One of the most common network attack vectors is to compromise a user workstation through internet-based malware, escalate privileges to the local administrator level, then escalate again to the domain (within AD) administrative level. By excluding users' workstations and network accounts from the Enterprise Email AD, this entire process is short-circuited. Further, the consolidation of email services and attributes into a single, dedicated AD facilitates the use of a best-practice out-of-band network for administration.

Achieving these benefits required development of a modified authentication mechanism. In order to increase security and reduce the complexity of interoperability strategies across a diverse network topology, the new authentication mechanism had to be independent of local directory services currently deployed within the Army and DoD. Because DoD primarily used Microsoft Exchange for email and CAC-based PKI certificates for two-factor authentication, DoD asked Microsoft in February 2009 to make software changes to Exchange and Outlook to enable an alternate authentication method using CAC-based PKI certificates that would work across AD boundaries.

To further enhance the security of the alternate authentication method, the DoD specified that the authentication process must happen encapsulated in a Transport Layer Security (TLS) encrypted tunnel. (TLS is an upgrade to the previous Secure Sockets Layer 3.0 protocol/cipher and allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.) Microsoft responded by working closely with DISA and the Army to develop and test new functionality in Microsoft Exchange 2010 and Microsoft Outlook 2007 to support TLS-encrypted, cross-boundary CAC authentication. Microsoft implemented this design change to its commercial products at no cost to the Department of Defense or Department of the Army.

Workstation Baseline Updates

The PKI certificate authentication capability includes specific configuration requirements and a minimum baseline for each workstation. The enhanced authentication capability will not work on a Windows XP machine because the security underpinnings of XP are not robust enough to provide the necessary functionality. Therefore, users must have either Windows Vista or Windows 7 on their desktop/laptop. Additionally, patches/updates for the operating system, ActivClient (the current smartcard support software), Tumbleweed (the current certificate verification software) and Outlook are required to fully enable the capability. Each of those patches, as well as a variety of configuration policies and settings, had to be applied to every workstation that would be used for Enterprise Email access across the Army.

During the early migrations to Enterprise Email, the Army exposed some deficiencies in desktop management that posed challenges to meeting this baseline configuration. The Army used this opportunity to improve its desktop configuration management strategies, benefiting both the Enterprise Email efforts and the overall health of the network.

Additionally, it is important to note that the Army views the lack of backwards-compatibility with the Windows XP operating system to be a non-issue, or perhaps a benefit/incentive. Knowing the security vulnerabilities inherent in Windows XP, and understanding that Windows XP is nearing obsolescence, Army policy for some time has mandated removal of Windows XP from the inventory as soon as practical.

Bandwidth

Concerns regarding the need to increase network bandwidth to accommodate a cloud-based service were significantly mitigated by using DISA as the managed service provider. Moving from a locally hosted email service to a private cloud solution places additional burden and importance on global network connectivity. During the planning phase of the Enterprise Email implementation, the Army and DISA performed a bandwidth analysis of Army locations across the CONUS and OCONUS theaters. Minimum bandwidth and redundancy requirements were established based on each location’s user population and existing network capacity. These metrics and criteria were used to develop an upgrade plan, ensuring sufficient capacity to support Enterprise Email. In some locations, the criteria resulted in the best option being the locally positioned, DISA-owned/operated email server infrastructure.

The Army already obtains the majority of its bandwidth from DISA. By working closely with DISA as both the telecommunications network provider and the provider of Enterprise Email, network connectivity was optimized at minimal cost. For fiscal year 2012, expanded bandwidth increased the Army’s long-haul communications bill by approximately $1.4 million, to approximately $313 million. An additional annual increase by $180,000 is expected starting in FY 2013 on the classified network. Note that recurring bandwidth costs are funded separately from the Enterprise Email program.

Migration Tools

Migrating from the Army's existing diverse email infrastructure to the consolidated DISA-hosted solution generated a unique set of requirements. Migration mandated moving mailbox data across security boundaries without the use of cross-forest trusts, while simultaneously resolving multiple identities to the new persona-based enterprise identity paradigm. In order to quickly and efficiently migrate 800,000 business-class users, the Army needed a migration tool that was robust, scalable and affordable.

In response, the Army leveraged the Enterprise Directory Services – Provisioning (EDS-P) tool. EDS-P was developed by the Army's Software Engineering Center at Communications-Electronics Command to support brigade combat teams in moving mail from an Exchange server in one environment to an Exchange server in another environment (most often during deployments). This existing tool contained the framework to handle user migrations and identity mapping, but required an update to include support for moving to the DISA Exchange 2010 cloud.

Pilot migrations uncovered distinct operational and performance challenges in the initial version of the updated tool. Army Network Enterprise Technology Command (NETCOM) worked with the EDS-P developers and partners to revise and improve EDS-P through software updates and changes to the underlying framework. The resulting version is able to migrate thousands of users each night from multiple locations into the DISA Exchange 2010 cloud.

Local National/Foreign Military/Volunteer Users

The requirement for CAC authentication raised the issue of support for authorized users who are not issued a CAC due to their status as a local national, foreign military or other unique situation, such as Red Cross volunteers. Some countries' sovereignty laws prevent the United States from capturing biometric data, which is required for CAC issuance. Without a CAC, DMDC has no record of the individual; thus there is no enterprise identity and no method by which DISA can provision an email account. The Army worked with DISA and DMDC to identify current procedures for computer access via alternate smartcard tokens, and developed a long-term solution for every possibility in foreign countries and among volunteers that will produce DoD records and enterprise DoD identities for each individual. Due to the time required to implement the long-term solution, an interim solution using existing alternate smartcard tokens was developed to provide an immediate capability.

PART 2 – SECURITY ASSESSMENT OF THE SELECTED APPROACH

Security Assessment Summary:

Unclassified email by its common definition is not a command and control system. However, its importance to the Army, as well as other DoD components, cannot be minimized: it is a critical mission enabler that serves as the primary means for communications at all levels within the Department. The ability to ensure reliability and availability of this communications mechanism; to monitor, detect and react to vulnerabilities and threats; and to enable safeguards and protections formulated according to intelligence-based activities is critical. Security becomes even more important as the use of smart-phones and other mobility-enabled devices takes hold across the Department. The security design must not only protect the internal email infrastructure itself and the data stored within the infrastructure, but also provide protection from malicious or otherwise dangerous content to workstations and mobile and other user-based devices. The Army, in its initial requirement to DISA, specified Enterprise Email be at Mission Assurance Category (MAC) II. DISA, anticipating more stringent requirements to support other DoD/Joint agencies, built the DoD Enterprise Email service to comply with the highest category, MAC I.

Over the summer/fall of 2011, DISA initiated a comprehensive security review of Enterprise Email, engaging the National Security Agency (NSA) to partner in the project. The effort began with a focused review of the Enterprise Email security architecture by the NSA Architecture Group and the DISA Security Architecture Analysis Team/Penetration Testing (SAAT/PT) team. This multi-week effort concluded that the overall design and architecture were well structured. It also aided in devising tests for the onsite infrastructure assessment phase.

The onsite assessment was supported by an NSA Blue Team and a combination of the DISA SAAT/PT team and DISA Certification Support personnel. This multi-week effort included reviewing both a full Enterprise Email pod (infrastructure components supporting Enterprise Email) housed within a DISA Enterprise Computing Center (DECC) and a mini-pod, which is used in instances where mission requirements warrant a “localized” installation of email capabilities. Further operational analysis looked at capabilities for monitoring and reacting to threats and attacks. While the review did identify implementation-level issues and procedural items that must be addressed, it found no general architectural issues, further validating that the overall security design of the system is sound. In fact, at the conclusion of the onsite assessment, a member of the NSA team indicated that the security of this system was one of the strongest he had seen, a testament to the overall emphasis on security.

DISA engineers are using the assessment results to remediate identified issues, as well as to strengthen the security of Enterprise Email through expanded capabilities and improved procedures. Unlike traditional distributed implementations, changes can be effected in a structured manner on all systems by the operations support team, improving security across the true enterprise. To further validate the effectiveness of the improved infrastructure and personnel supporting Enterprise Email operations/security, DISA plans to conduct a red team assessment in 2012. A red team approach will test Enterprise Email in a more real-world "unannounced" scenario, evaluating both capabilities and processes. Such efforts, coupled with a continuous monitoring approach, provide a basis for reliable, secure email services.

Key Security Advantages over the Status Quo:

DISA's instantiation of Enterprise Email provides a high level of security, with an architecture that takes advantage of the strong practices and security controls provided by DISA's Computing Services operations and enhancements inherent in the Enterprise Email design. The solution also addresses unique DoD requirements not typical of commercial operations that are critical to providing reliable and secure operations. The following paragraphs provide an overview of the key security advantages of the Enterprise Email design and highlight factors specific to DoD operations.

Ability to enable strong assurances of user identity through trusted and reliable authentication processes.

Authentication techniques such as userid/password combinations create considerable risks for important business systems. Techniques that rely on multi-factor authentication greatly reduce the risk of compromise and provide a higher assurance of the user's identity. Authentication that only occurs in a TLS-encrypted tunnel further reduces the risk of compromise. The DISA design for DoD Enterprise Email utilizes the DoD PKI and digital certificates issued on the CAC as the means of controlling access to the system, and conducts authentication using TLS encryption. Enterprise Email maintains the directory of users and their privileges by leveraging the authoritative data source for CAC and certificate issuance managed by DMDC. In the event of a compromised certificate, DoD PKI provides an ability to revoke certificates at the enterprise level, enabling quick disabling of the certificate in Enterprise Email.

Reduced risk through separation of a user's email attributes from the attributes and privileges afforded through the user's home network environment.

Microsoft's Active Directory (AD) construct serves as a central location for network administration and security. It supports authenticating and authorizing all users and computers within a network of Windows domain type, assigning and enforcing security policies for all computers in a network, and installing or updating software on network computers. To eliminate risks to Enterprise Email that could be inherited through rules and permissions managed at a local installation, a separate AD infrastructure, referred to as the Enterprise Application and Services Forest was established and modifications made to support the use of this separate, well-structured, limited-function AD construct.

Strong controls for limiting access to authorized users responsible for administration of the Enterprise Email infrastructure.

The ability to effect change to a system creates risk that must be tightly controlled. Systems administrators and operations support personnel typically require elevated privileges to perform their duties. To mitigate this risk, best practices involve using an “out-of-band” (OOB) – or off the main production network – technique for performing system administration. This approach essentially supports blocking all administrative access through the in-band network, thus dramatically reducing the attack surface for administration-based risks. DISA has institutionalized the use of an OOB network across the DECC and Computing Services infrastructure for all systems administration. This specialized network has strong authentication capabilities with extensive logging and the ability to limit the systems that an OOB user would be authorized to access. Both DISA systems administration personnel and authorized Army Blackberry administrators use the OOB network as the vehicle to execute their administrative duties. Because personnel with elevated privileges present a greater risk, all those who require OOB network access have DoD security clearances with appropriate background investigations.

Effective configuration and change control processes that allow for timely application of security patches/fixes and other system maintenance.

Vendors continuously publish patches and updates to their software. Whether the updates address security-related issues or functionally related bugs, or implement new capabilities, it is critical that robust mechanisms exist to manage change. DoD uses the Information Assurance Vulnerability Management process to provide notification and direction to the systems administration community regarding security-related vulnerabilities. Using the information and guidance provided by U.S. Cyber Command, DISA develops implementation plans (with a special emphasis on “alerts”). Where possible, DISA uses a “round-robin” construct to pull a system out of the operational configuration, update it and return it to the operational configuration. This effort continues until all systems are appropriately patched. In instances where a round-robin technique cannot be used (*e.g.,* when there is no failover device), the Authorized Service Interruption process is used to schedule outage time to address the risk. Through centralized control of the infrastructure, the risk of unpatched, and therefore vulnerable, systems is greatly reduced.

DoD-Specific Requirements:

Ability to isolate elements of the network, to include full disconnect from the Internet, in the event of a cyber threat.

The sophistication of cyber-based threats and adversary capabilities continues to increase. As threats are identified and analyzed, mitigations must be developed and implemented quickly. The reliance on email necessitates an ability to implement enterprise-level mitigation and to continue operations if a full disconnect from the Internet is warranted. The Enterprise Email design, coupled with the security architecture of the Non-classified Internet Protocol Routing Network (NIPRNet), provides capabilities for isolating the high-risk network segments while enabling continued use of email. At the connection points between the NIPRNet and the Internet, DISA has instituted a number of capabilities that can limit external risks, including Intrusion Detection Systems, firewall capabilities and web content filtering. Because Enterprise Email is fully contained inside the NIPRNet boundary, the system can remain functional in the event of the most serious of threats.

Ability to protect, detect and react to adversarial and otherwise malicious actions.

Enterprise Email provides a layered defense mechanism designed to protect both the information within the Enterprise Email infrastructure and the user devices that receive and store data sent via Enterprise Email. Protections at different levels of the infrastructure provide a defense-in-depth construct that affords a higher degree of security.

- Gateway: Capabilities implemented at the Internet boundary through solutions such as network sensors, Web Content Filtering and the Email Security Gateway support the monitoring and inspection of traffic originating from the Internet, including Outlook Web Access and messages sent from an external organization (*e.g.,* a .com entity).

- Enterprise Email Infrastructure: The Enterprise Email infrastructure was hardened using techniques outlined in various DoD Security Technical Implementation Guides. These documents outline standards and processes for securing/hardening servers, networks and mobile devices across the Department. Additional layers of security are enabled through the Host-Based Security System (HBSS), which provides anti-virus, white-listing of trusted programs and intrusion detection for the infrastructure itself. Enterprise Email also currently uses McAfee Security for Microsoft Exchange (MSME), which inspects email traffic for malicious content. For Enterprise Email, MSME monitors traffic that originates within the DoD network, performing inspection/control before allowing content to go to the host level.

- Host Level: USCYBERCOM has mandated HBSS implementation and use to provide anti-virus and intrusion detection/prevention at the workstation level. These capabilities add a layer of protection at the lowest level in the architecture.

Each tool/capability generates data that can be used to monitor Enterprise Email. Through log collection and correlation analysis systems, network assurance analysts can monitor the infrastructure for threats and attacks. By fusing this data with classified intelligence data (as well as other unclassified non- Enterprise Email data sources), analysts are postured to detect potential adversarial activities and implement techniques to safeguard the enterprise from such activities.

Ability to take effective steps in addressing negligent disclosure of classified information, including the ability to track and delete messages.

Systems that manage the entry of free-form information, such as email or document management systems, depend primarily on the user to assert the classification of data being entered into the system. Unfortunately, users do make errors and suspected classified information is mislabeled. In these situations, actual classification must be determined swiftly, and systems administration and security professionals must take actions required to contain the information and execute appropriate cleansing procedures. The Enterprise Email design enables search and delete capabilities across the entire infrastructure, as well as the tracking of messages sent outside Enterprise Email. All DISA's Enterprise Email administrators and security professionals possess a security clearance with appropriate background investigations.

6. CERTIFICATION OF SELECTED APPROACH

Section 353 requires the Secretary of the Army to certify that the approach selected for moving forward with Enterprise Email is in the best technical and financial interests of the Army and provides for the maximum amount of competition possible in accordance with 10 USC § 2302(3)(D).

The Army has for many years delivered IT services and capabilities in a decentralized fashion, making it difficult to achieve enterprise-wide financial transparency and effective interoperability across various technology domains. The Army is now in the process of transforming its core IT capabilities in order to create a consolidated IT infrastructure.

As previously noted, the Army is obtaining Enterprise Email capabilities as a managed service through an interagency acquisition with DISA. Interagency acquisition transactions are based on statutory authority and provide legitimate means for agencies to acquire goods or services from other agencies that have the capabilities and expertise to provide those goods or services.

DoD's Enterprise Email service has enabled the Army to quickly leverage existing capabilities to support the Army's transformation objectives. The Army was able to utilize DISA's scalable capacity, redundancy, improved security, robust information assurance and responsive end-to-end operations, including integration into the DoD Enterprise Directory.

The consolidation of email into this Enterprise service from DISA is in the best technical and financial interest of the Army because the DISA solution provides the lowest security risks with the highest benefits of leveraging DISA's robust geo-redundant infrastructure and its interoperable components. The solution leverages existing Army-owned software licenses at the lowest cost and produces significant cost savings.

DISA, as the “service provider” for email messaging for the Army, has the enduring legal obligation to obtain the maximum amount of competition at the various levels of hardware, licensing and service contracts, as required by law and regulation. DISA has a long track record of openly competing requirements to ensure maximum competition in providing enterprise-wide capabilities.

Attachment 3 to this report is a list of DISA contracting vehicles that support the Enterprise Email service, including the type of competition for each contract. Generally, the Capacity and Professional services categories of contracts have been awarded under full and open competition, with some Section 8(a) contract awards when appropriate. Most of the utility-type contracts, which acquire specific brand-name software licenses based on agency standardization decisions or architecture network standards, have been competed among responsible sources that are in the business of providing those brands of software licenses.

The Army’s adoption of DoD’s Enterprise Email service leveraged existing programs, capabilities and services that had previously been acquired competitively by DISA. DoD Enterprise Email for the Army also utilized existing Army Microsoft licenses, which previously had been disparately managed across the Army. The consolidation and use of existing licenses at the enterprise level did not require a new contracting action and was in compliance with statutory competition requirements. To date, DISA has expended $525 million establishing Enterprise Services Centers that enable delivery of services such as Enterprise Email, with maximum use of competitive contracts:

Competition Type	% Funds Expended
Full and Open	88
Small Business 8a Set-Aside	6.5
Brand Name Competition	2

The statutory and regulatory competition requirements are accomplished at the DISA service provider level on contracts for hardware, software licensing, and support services. Competition is mostly done under a full and open competition, with a limited amount of small business or brand name competition when appropriate, to provide for the maximum amount of competition possible in accordance with 10 USC § 2302(3)(D). This information supports the conclusion in the AAE’s acquisition decision memorandum issued on 3 February 2012; a copy is at attachment 4 to this report.

7. FUNDING

Section 353 of the NDAA requires a detailed accounting of the funding expended by the program as of the date of enactment (December 31, 2011), as well as an estimate of the funding needed to complete the selected approach.

Summary: Through December 31, 2011, the project expended $71,739,765.33. The estimated amount to reach full operational capability on September 30, 2012, with the balance of the deferred migrations finished by March 31, 2013 is $54,693,111.

Thereafter, annual recurring costs are as predicted in the cost-benefit analysis with updates by AAA: $298.2M from FY13-17 (when adjusted to then-year dollars). It should also be noted that the project is executed by DISA using working capital funds, and minor year of execution adjustments are anticipated. Additionally, the operation of a formal program office within the Program Executive Office, Enterprise Information Systems, is anticipated to cost approximately $1.004M per year after the project reaches full operational capability. NETCOM remains responsible for direct support to Army users and for conducting network operations.

<u>Expenditures through December 31, 2011</u>: $71,739,765

1) Migration funding

Organization	Description	Total cost
CIO/G-6	Fly-away support teams & Brigade Migration Command Center (BMCC) support – labor	5,102,919.93
	Fly-away support & BMCC support – travel	225,349.40
NETCOM	EDS-P migration tool upgrade	869,596.00
	Migration support – contract labor & travel	2,036,584.00
	Migration support – government travel	715,964.00
	Civilian overtime	89,997.00
Sub-Total		**$9,040,410.33**

2) Operational funding to DISA

Project (network)			Amount
NIPRNET	Startup/migration costs		**53,899,355**
SIPRNET	Startup/migration costs		**8,800,000**
Sub-Total			**$62,699,355**

Estimate to Complete Selected Approach: $54,693,111

1) **Projected project management funding required to establish a formal program management office and to provide formal acquisition oversight through September 30, 2012, of the remaining Army Enterprise Email activities**

Organization	Description	Total cost
PEO-EIS	Enterprise Email Program Management Office	$1,325,280

2) **Funding required to complete originally scheduled NIPRNET migrations (195,963 Exchange migrations plus 400,000 AKO migrations)**

Organization	Description	Total cost
CIO/G-6	Fly-away teams/BMCC support – labor	1,812,738.43
	Fly-away teams/BMCC support – travel	178,858.33
NETCOM	Migration support – contract labor & travel	2,451,452.88
	Migration support – government travel	78,562.79
	Civilian Overtime	18,323.44
Sub-Total		**$4,539,935.88**

3) **Funding required to complete organizations not on original NIPRNET schedule (440,188 Exchange migrations)**

Organization	Description	Total cost
CIO/G-6	Fly-away teams/BMCC support – labor	1,256,070.73
	Fly-away teams/BMCC support – travel	123,933.33
NETCOM	Migration support – contract labor & travel	1,698,644.52
	Migration support – government travel	54,437.21
	Civilian overtime	12,696.56
Sub-Total		**$3,145,782.35**

4) **Funding to complete SIPRNET migrations (200,000 Exchange migrations)**

Organization	Description	Total cost
CIO/G-6	Fly-away teams/BMCC support – labor	570,941.24
	Fly-away teams/BMCC support – travel	342,127.50
	Nonrecurring charges for circuit upgrades	10,000.00
	Cryptographic hardware for circuit upgrades	77,000.00
NETCOM	EDS-P tool upgrade/support	671,128.00
	Migration support – contract labor & travel	1,592,296.63
	Migration support – government travel	348,000.00

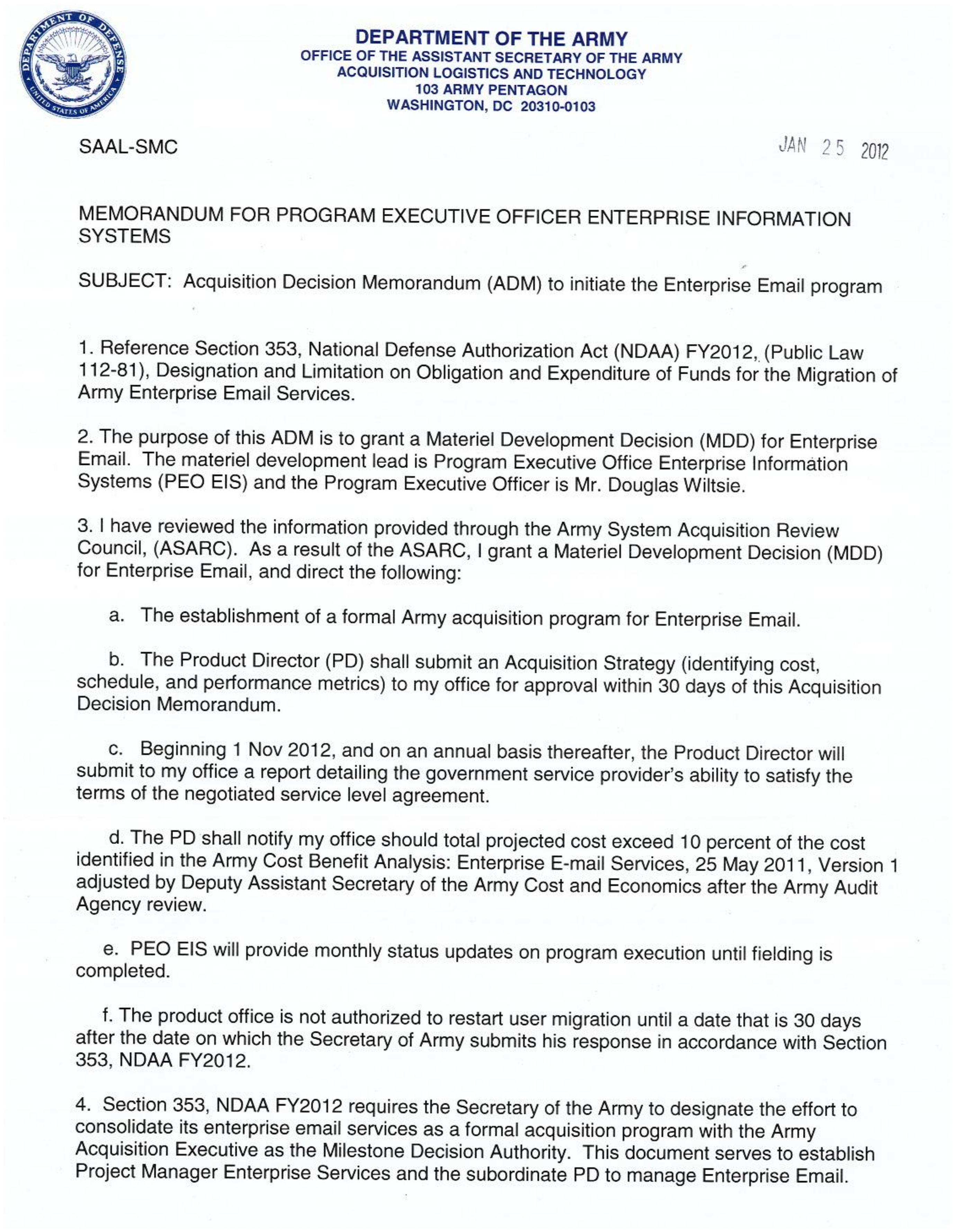
	Civilian overtime	87,120.00
Sub-Total		**$3,698,613.37**

5) Funding to Sustain Service through September 30, 2012

Organization	Description	Total cost
DISA	Operation and maintenance	$41,983,500.00

ATTACHMENTS:

1. Acquisition Decision Memorandum, January 25, 2012
2. Army Audit Agency Report, January 19, 2012
3. Defense Information Systems Agency Contract Vehicles
4. Acquisition Decision Memorandum, February 3, 2012
5. Acronym List



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON, DC 20310-0103

SAAL-SMC

JAN 25 2012

MEMORANDUM FOR PROGRAM EXECUTIVE OFFICER ENTERPRISE INFORMATION SYSTEMS

SUBJECT: Acquisition Decision Memorandum (ADM) to initiate the Enterprise Email program

1. Reference Section 353, National Defense Authorization Act (NDAA) FY2012, (Public Law 112-81), Designation and Limitation on Obligation and Expenditure of Funds for the Migration of Army Enterprise Email Services.

2. The purpose of this ADM is to grant a Materiel Development Decision (MDD) for Enterprise Email. The materiel development lead is Program Executive Office Enterprise Information Systems (PEO EIS) and the Program Executive Officer is Mr. Douglas Wiltsie.

3. I have reviewed the information provided through the Army System Acquisition Review Council, (ASARC). As a result of the ASARC, I grant a Materiel Development Decision (MDD) for Enterprise Email, and direct the following:

a. The establishment of a formal Army acquisition program for Enterprise Email.

b. The Product Director (PD) shall submit an Acquisition Strategy (identifying cost, schedule, and performance metrics) to my office for approval within 30 days of this Acquisition Decision Memorandum.

c. Beginning 1 Nov 2012, and on an annual basis thereafter, the Product Director will submit to my office a report detailing the government service provider's ability to satisfy the terms of the negotiated service level agreement.

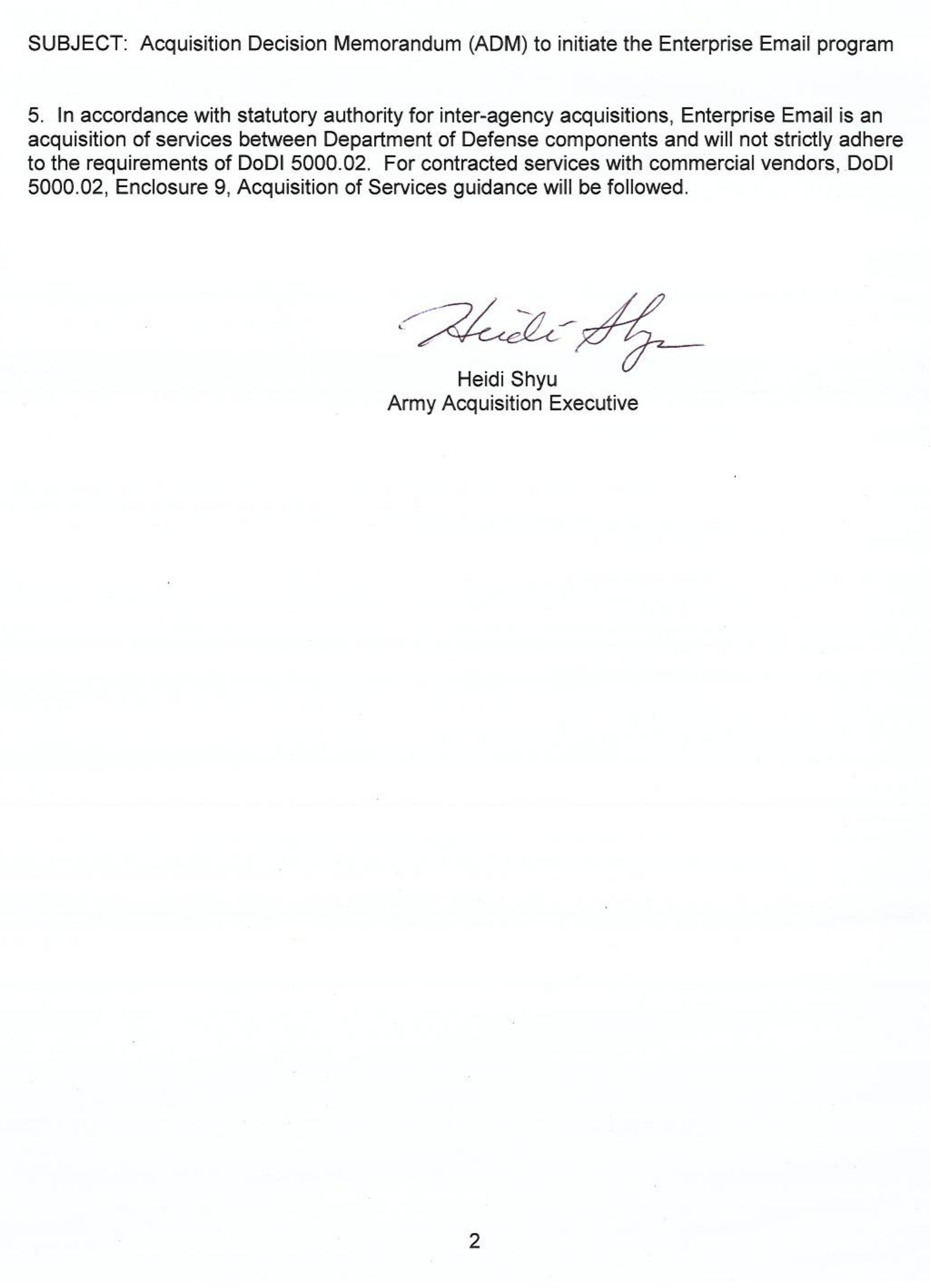
d. The PD shall notify my office should total projected cost exceed 10 percent of the cost identified in the Army Cost Benefit Analysis: Enterprise E-mail Services, 25 May 2011, Version 1 adjusted by Deputy Assistant Secretary of the Army Cost and Economics after the Army Audit Agency review.

e. PEO EIS will provide monthly status updates on program execution until fielding is completed.

f. The product office is not authorized to restart user migration until a date that is 30 days after the date on which the Secretary of Army submits his response in accordance with Section 353, NDAA FY2012.

4. Section 353, NDAA FY2012 requires the Secretary of the Army to designate the effort to consolidate its enterprise email services as a formal acquisition program with the Army Acquisition Executive as the Milestone Decision Authority. This document serves to establish Project Manager Enterprise Services and the subordinate PD to manage Enterprise Email.

Attachment 1 – Acquisition Decision Memorandum, January 25, 2012



SUBJECT: Acquisition Decision Memorandum (ADM) to initiate the Enterprise Email program

5. In accordance with statutory authority for inter-agency acquisitions, Enterprise Email is an acquisition of services between Department of Defense components and will not strictly adhere to the requirements of DoDI 5000.02. For contracted services with commercial vendors, DoDI 5000.02, Enclosure 9, Acquisition of Services guidance will be followed.

Heidi Shyu

Heidi Shyu
Army Acquisition Executive

DEPARTMENT OF THE ARMY
U.S. ARMY AUDIT AGENCY
OFFICE OF THE DEPUTY AUDITOR GENERAL
FINANCIAL MANAGEMENT & COMPTROLLER AUDITS
3101 PARK CENTER DRIVE
ALEXANDRIA, VA 22302-1596

SAAG-FMT 19 January 2012

MEMORANDUM FOR Army Chief Information Officer/G-6

SUBJECT: Attestation Review of Enterprise E-mail Cost-Benefit Analysis (Project Number A-2012-0259.000), Report: A-2012-0047-FMT

1. **Introduction.** This memorandum report presents the results of our attestation review of the enterprise e-mail cost-benefit analysis (CBA). We performed this review in response to the National Defense Authorization Act of 2012, which tasks our Agency to evaluate expected cost savings and cost avoidance from each of four alternatives being considered for enterprise e-mail.

2. **What We Audited**. We assessed costs reported in the Army CBA for enterprise e-mail services dated 25 May 2011 and approved by the Deputy Assistant Secretary of the Army for Cost and Economics on 8 June 2011. In accordance with the language in the National Defense Authorization Act, we focused solely on statements in the analysis specifically related to the costs of the four alternatives; we didn't review non-quantifiable benefits, selection criteria, or overall selection.

3. **Auditing Standards**. We conducted this attestation review engagement in accordance with generally accepted government auditing standards, which incorporate attestation standards established by the American Institute of Certified Public Accountants. An attestation review consists of sufficient testing to express a conclusion about whether any information came to the auditors' attention on the basis of the work performed that indicates the assertion (in this instance, the CBA) is not presented or not fairly stated in all material respects based on the criteria. An attestation is appropriate for evaluating cost-benefit analyses. We selected a review attestation because of the limited time allotted to perform the effort.

4. **Scope and Methodology**. To determine if cost estimates for the four options were presented fairly in all material respects, we judgmentally selected a limited number of high-impact cost drivers. We traced costs through work breakdown structures to obtain supporting documentation for the individual cost drivers. We also analyzed how the drivers were applied, the methodology that was used to calculate overall costs for the four options, and reported cost savings. We found minor discrepancies in multiple calculations, but none of them individually or taken together had a material

effect on CBA costs. We relied heavily on opinions of subject matter experts presented in the supporting documentation; we don't have the technical expertise to verify that the supporting documentation accurately reflected a solution that would successfully provide for enterprise e-mail.

5. **Results of Review**. We found no material issues with the four alternatives presented; however, we believe the projected cost savings don't include all necessary factors. As a result, the savings, though still significant, were overstated. Our results on the four alternatives and the overall cost savings as reported in the CBA follow.

a. **Status Quo.** We believe the estimated costs reported in the CBA were sufficiently reliable to inform the decision, though we don't believe the methodology used to create the cost estimate thoroughly reflected the status quo. We identified two primary issues with the status quo costs.

(1) The Chief Information Officer (CIO)/G-6 used limited data inputs from a very small population to develop a per-user cost and extrapolated this information across the entire Army. A larger pool of data would project costs across the Army more accurately. Because of our concern over the methodology, we conducted a separate analysis of previous Agency audit work related to funding baseline information technology services. Specifically, we calculated the cost of providing baseline e-mail services at the installation used in the CBA (Redstone Arsenal). We determined the baseline service cost for each 100MB mailbox was about $114 in FY 08. Based on the $114 for baseline services, we determined that the per-user cost used in the CBA ($142 plus ancillary costs) as the status quo estimate for a 1GB mailbox was sufficiently reliable to inform the decision.

(2) As part of the status quo calculation, an "as-is" cost of $20.1 million for Army Knowledge Online (AKO) was included. We couldn't obtain sufficient support for this figure. AKO provided support for about $12.2 million in "as-is" costs. We don't believe the difference between the CBA and the support we were provided materially affects the status quo calculation; the difference is only 4 percent of the original "as-is" cost of $1,366.4 million. We address the effect of this variance on overall cost savings in paragraph 5e.

b. **Commercial Vendor.** We believe the methodology and costs reported in the CBA for this option were sufficiently reliable to inform the decision except for potential future costs related to licensing Outlook Web Access software. We obtained sufficient documentation from CIO/G-6 to support the work breakdown structure; the support relied heavily on subject matter expertise. The estimated cost of Outlook Web Access client access licenses and 3 years of software assurance was added to the work breakdown structure to produce the overall cost of this option. Costs for the licenses and assurance were supported and calculated accurately in all material respects; however, the lack of software assurance over the final 4 years of the CBA timeframe adds risk to the reliability of the cost estimate for the commercial option. As such, to maintain a conservative approach in calculating costs, the analysis should have included additional costs after the initial 3-year software assurance coverage. If the costs were unknown, this should have been addressed in the analysis by stating there was an unknown future cost. Based on information and feedback from representatives from the Army's designated source for commercial information technology—Computer Hardware, Enterprise Software and Solutions—we believe this omission underestimated this option by a range of about $11.9 million to $23.9 million over the 7 years, which only represents about 4 percent of the original estimate of $543.7 million.

c. **Army Knowledge Online.** We believe the methodology and costs reported in the CBA for this option was sufficiently reliable to inform the decisions. We obtained sufficient documentation from Project Manager (PM)-AKO to support the work breakdown structure. The documentation relied heavily on subject matter expertise. We found that the work breakdown structure didn't include costs for journaling under this option. Previous versions of the AKO work breakdown structure included about $1.5 million over the period covered in the analysis for this function, which is less than 1 percent of the estimated $237.1 million cost of this option. We also evaluated the accuracy of two statements in the Summary of Alternatives Considered related to costs.

(1) The summary states that AKO's lack of BlackBerry support is a significant challenge. While AKO doesn't support the BlackBerry brand of mobile devices, we found that the cost of developing and providing that support is included in the work breakdown structure.

(2) The summary states that the cost of making AKO support Public Key Infrastructure (PKI) certificate authentication from Outlook was unspecified. Based on discussions with CIO/G-6 and PM-AKO personnel, AKO wasn't providing this function and the cost to develop it was unknown when the CBA was originally developed in 2010. However, as of the 25 May 2011 date of the published CBA, PM-AKO personnel told us that AKO was capable of providing this function. They weren't able to define the costs they incurred to provide this function.

d. **Defense Information Systems Agency.** We believe the methodology and costs reported in the CBA for this option were sufficiently reliable to inform the decision, except for potential future costs related to licensing Outlook Web Access software. This is the same exception that was noted with the commercial vendor alternative discussed earlier. We obtained sufficient documentation from the Defense Information Systems Agency (DISA) to support the work breakdown structure; the support relied heavily on subject matter expertise. We also reviewed the DISA option costs added by Deputy Assistant Secretary of the Army for Cost and Economics to allow for migration, functionality for the secure Internet protocol router network (SIPRNet), and licensing. Costs for migration and SIPRNet functionality were appropriate. However, just as with the commercial option, licensing costs only included 3 years of software assurance. To reduce cost risk and maintain a conservative approach in calculating costs, the CBA should have included additional costs after the initial 3-year software assurance coverage. At a minimum, this should have been addressed in the analysis by stating there was a future cost but the cost was unknown. We believe this omission underestimated this option by a range of about $11.9 million to $23.9 million over the 7 years, which only represents about 5 percent of the original estimate of $442.5 million.

e. **Cost Savings.** We don't believe the methodology and savings reported in the CBA were sufficiently reliable primarily because the methodology didn't account for unrecoverable enduring costs for any of the options presented. Based on documentation provided to us, projected savings, though still significant, were overstated.

(1) **Cost Savings Reflected in CBA**. The cost savings are presented in the CBA in the summary and recommendation sections. The CBA states simply that the DISA option will save the Army well over $100 million per year from FY 13 on. Accordingly, we only evaluated cost savings from FY 13 to FY 17. CIO/G-6 made this determination by subtracting the cost estimate for the status quo option by the cost estimate for the DISA option, as shown on this chart:

FY 11 $M	FY13	FY14	FY15	FY16	FY17	Total
Status Quo	$195.2	$195.2	$195.2	$195.2	$195.2	$976.0
DISA Option	$55.1	$52.7	$50.5	$48.6	$45.3	$252.2
Projected Savings	$140.1	$142.5	$144.7	$146.6	$149.9	$723.8

(2) **Verification of Cost Savings**. We could not verify these savings based on the documentation provided to us. As discussed in paragraph 5a regarding the status quo alternative, we could not support all of the costs related to current AKO costs. That, along with minor mathematical corrections, reduced total costs for the status quo option by about $8.1 million per year. As discussed in paragraph 5d regarding the DISA alternative, omitting the software assurance costs for the final 4 years of the CBA period underestimated this option by a range of about $11.9 million to $23.9 million over the 7 years. More significantly, these savings projections don't account for any unrecoverable enduring costs for the Microsoft Exchange structure or AKO e-mail functionality to support non-common access card (CAC) holders (such as retirees and family). Documentation provided by CIO/G-6 during our review estimates that 25 percent of the Exchange costs—representing personnel, space, and power usage—would be unrecoverable since these costs can't be reduced or removed completely. CIO/G-6 estimated that the AKO enduring costs would be $12.8 million per year, but we used about $12.2 million to account for the reduction in the total AKO e-mail costs reflected in the status quo. While we agree the enduring AKO cost is most likely less than the AKO cost in the status quo, we were unable to determine an appropriate factor to apply. These unrecoverable costs would need to be applied equally to the commercial, AKO, and DISA options.

(3) **Adjusted Cost Savings**. With the adjustments to the status quo and DISA options and including unrecoverable costs, the savings would be about $76.1 million in FY 13, as shown on this chart:

FY 11 $M	FY 13	FY 14	FY 15	FY 16	FY 17	TOTAL
Status Quo	$186.3	$186.9	$187.5	$187.5	$187.5	$935.7
Less Unrecoverable Costs	$55.1	$55.7	$56.3	$56.3	$56.3	$279.8
Recoverable Costs	$131.2	$131.2	$131.2	$131.2	$131.2	$655.9
Less DISA Option	$55.1	$52.7	$74.4	$48.6	$45.3	$275.9
Projected Savings	$76.1	$78.5	$56.8	$82.6	$85.9	$379.9

Note: Some totals differ due to rounding of per year cost.

This chart is based on 1.6 million users, which was used as the basis for the CBA and is still considered the scope of the enterprise e-mail project. For FYs 13-17, the per-user cost for the status quo option would average about $117 per year and the per user cost for the DISA option would average about $34.5 per year.

In addition to calculating the projected cost savings for DISA, we applied the same methodology to the commercial and AKO options to show how those options would change based on our analyses. The projected cost savings are presented in the enclosure.

6. **Audits of Actual Savings and Information Technology Acquisition Processes.** Our Agency plans to continue its oversight of the enterprise e-mail program. In November 2011, we announced an audit of enterprise e-mail with two objectives:

- To verify the Army maximized its efficiencies through use of enterprise e-mail.

- To verify that enterprise e-mail improved services to Army clients and performance metrics were tracked.

We expect to start this audit in February 2012. In addition, in response to concerns from the Defense Armed Services Committees, we plan to coordinate with the Assistant Secretary of the Army (Acquisition, Logistics and Technology) and CIO/G-6 to develop an audit that addresses information technology acquisition reform and potentially influences ongoing enterprise efforts within the Army, with the goal to identify lessons learned for the Army, as well as the other Armed Services and DOD.

7. **Acknowledgments.** These personnel contributed to the report: Thomas P. Robertson (Program Director); Leigh Ann Searight and Bruce Miller (Audit Managers); Carly Gifford (Auditor-in-Charge); and Tom Harvey, Jonathan Lee, and Yvette Rasnick (Auditors).

8. **Remarks.** I appreciate the courtesies and cooperation extended to us during the audit. This report isn't subject to the command reply process that AR 36-2 (Audit Services in the Department of the Army) prescribes.

FOR THE AUDITOR GENERAL:

Kevin F Kelly

KEVIN F. KELLY
Deputy Auditor General
Financial Management & Comptroller Audits

PROJECTED SAVINGS FOR ALTERNATIVES

COA 1 Status Quo

FY 11 $M	FY 13	FY 14	FY 15	FY 16	FY 17	TOTAL
Status Quo	$186.3	$186.9	$187.5	$187.5	$187.5	$935.7

For FYs 13-17, the per-user cost for the status quo option would be $117 per year.

COA 2 Managed Service Provided by a Commercial Vendor

FY 11 $M	FY 13	FY 14	FY 15	FY 16	FY 17	TOTAL
Status Quo	$186.3	$186.9	$187.5	$187.5	$187.5	$935.7
Less Unrecoverable Costs	$55.1	$55.7	$56.3	$56.3	$56.3	$279.8
Recoverable Costs	$131.2	$131.2	$131.2	$131.2	$131.2	$655.9
Less Commercial Option	$51.6	$58.2	$81.8	$78.3	$57.5	$327.4
Projected Savings	$79.6	$73.0	$49.4	$52.9	$73.7	$328.5

For FYs 13-17, the per-user cost for the commercial vendor option would average about $40.92 per year.

COA 3 Army Knowledge Online

FY 11 $M	FY 13	FY 14	FY 15	FY 16	FY 17	TOTAL
Status Quo	$186.3	$186.9	$187.5	$187.5	$187.5	$935.7
Less Unrecoverable Costs	$55.1	$55.7	$56.3	$56.3	$56.3	$279.8
Recoverable Costs	$131.2	$131.2	$131.2	$131.2	$131.2	$655.9
Less AKO Option	$28.0	$30.8	$40.3	$35.8	$27.4	$162.3
Projected Savings	$103.2	$100.4	$90.9	$95.4	$103.8	$493.5

For FYs 13-17, the per-user cost for the AKO option would average about $20.30 per year.

COA 4 Defense Information Systems Agency

FY 11 $M	FY 13	FY 14	FY 15	FY 16	FY 17	TOTAL
Status Quo	$186.3	$186.9	$187.5	$187.5	$187.5	$935.7
Less Unrecoverable Costs	$55.1	$55.7	$56.3	$56.3	$56.3	$279.8
Recoverable Costs	$131.2	$131.2	$131.2	$131.2	$131.2	$655.9
Less DISA Option	$55.1	$52.7	$74.4	$48.6	$45.3	$275.9
Projected Savings	$76.1	$78.5	$56.8	$82.6	$85.9	$379.9

For FYs 13-17, the per-user cost for the DISA option would average about $34.50 per year.

Note: In all tables, some totals differ due to rounding of per-year cost. Per-user costs are based on 1.6 million users and don't include FY 11 and FY 12 costs consistent with the CBA, which focused on savings from FYs13-17.

Our Mission

To serve America's Army by providing objective and independent auditing services. These services help the Army make informed decisions, resolve issues, use resources effectively and efficiently, and satisfy statutory and fiduciary responsibilities.

To Suggest Audits or Request Audit Support

To suggest audits or request audit support, contact the Office of the Principal Deputy Auditor General at 703-681-9802 or send an e-mail to AAAAuditRequests@conus.army.mil.

Additional Copies

We distribute each report in accordance with the requirements of Government Auditing Standards, GAO-07-731G, July 2007.

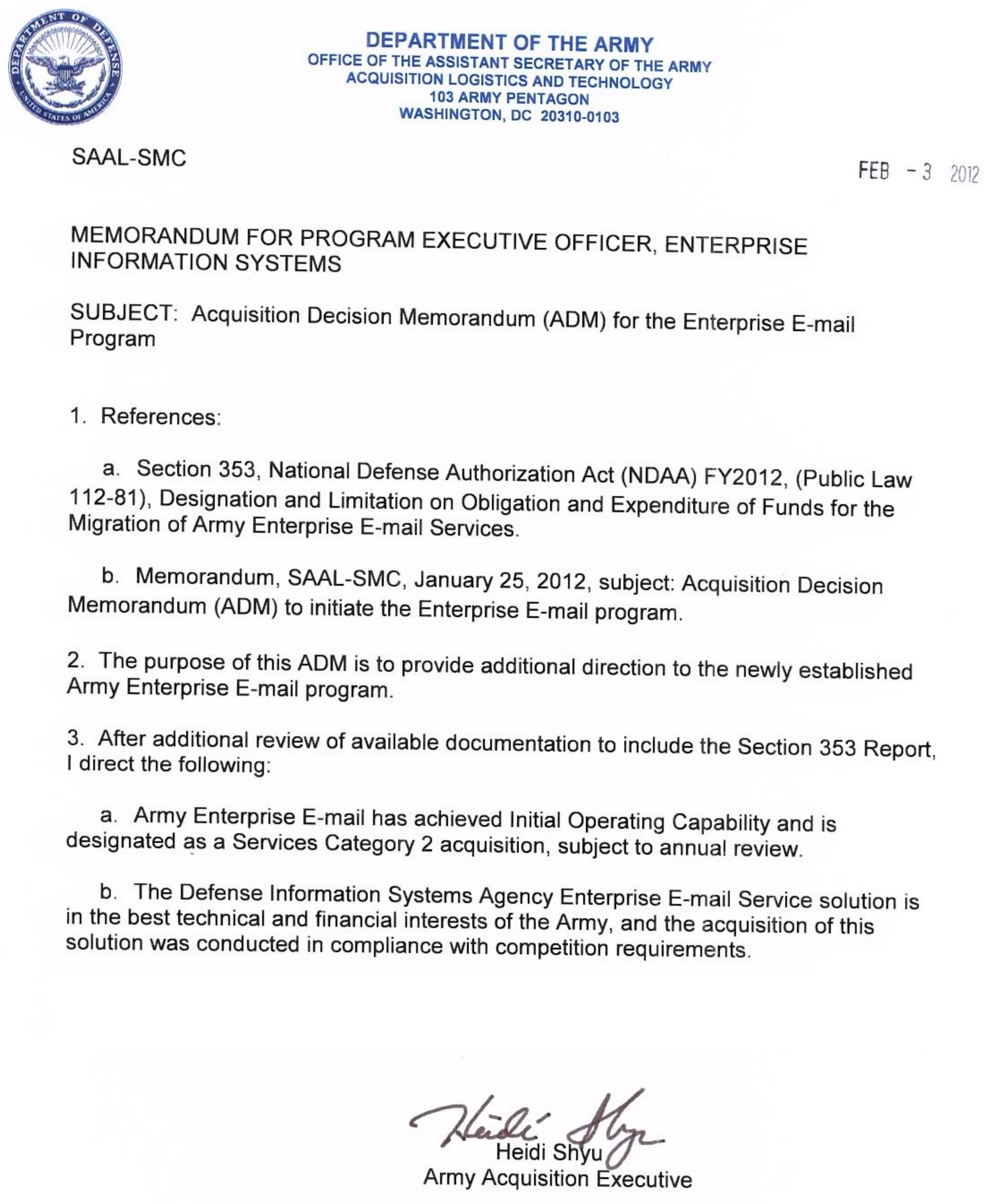
To obtain additional copies of this report or other U.S. Army Audit Agency reports, visit our Web site at https://www.aaa.army.mil. The site is available only to military domains and the U.S. Government Accountability Office. Other activities may request copies of Agency reports by contacting our Audit Coordination and Followup Office at 703-614-9439 or sending an e-mail to AAALiaison@conus.army.mil.

Defense Information Systems Agency Contracts, Part 1

CONTRACT #	AWARD DATE	EXP DATE W/ OPT YRS	CATEGORY	DESCRIPTION	CONTRACTOR	COMPETITION TYPE TITLE
HC1013-07-D-2004	01/25/07	09/30/12	Capacity	Capacity Services for HP Window/Linux	Hewlett-Packard Company	Full and Open
HC1013-07-D-2009	01/30/07	02/07/12	Capacity	Enterprise Storage Services	ViON Corporation	Full and Open
GS-35-F-0539J	05/23/07	10/31/11	Professional	Communications and Systems Engineering/Optimization/Consolidation	Network Connectivity Solutions Corp	Full and Open
HC1028-08-C-2012	05/29/08	01/31/12	Professional	DoD DMZ Support	Dynosi Government Services	Full and Open
HC1028-08-D-2008	01/07/11	01/06/12	Professional	Edge Computing for Enterprise Services	Network Connectivity Solutions Corp	Full and Open
HC1028-10-C-2016	04/29/10	05/13/15	Professional	SMC Mechanicsburg, Denver, CO, and Falls Church, VA Configuration	NOVA Corporation	Section 8(a) Set-Aside
HC1028-10-C-2022	06/25/10	06/30/15	Professional	Senior Program and Project Management Information Technology	KSJ & Associates Inc	Full and Open
HC1028-10-P-2035	01/29/10	01/31/12	Professional	DISA -OKC Unix Administrator tasks	Valdez International Corporation	Section 8(a) direct
HC1028-11-C-0115	06/08/11	06/14/16	Professional	Enterprise Email Operations Technical and Application Support	KNWEBS Inc	Full and Open
HC1028-11-D-0102	09/28/11	09/28/12	Capacity	Capacity Service for Communications	Knight Point Systems, LLC	Full and Open
HC1028-11-P-0131	12/09/10	12/14/12	Professional	Enterprise Email Operations Technical & Application Support Svcs	KNWEBS Inc	Section 8(a) direct
W912HZ-09-D-0003	12/13/10	12/14/11	Professional	Microsoft Support, Navy SharePoint 2007/2010	Eyak Technology LLC	Section 8(a) ANC
GS35F-0009M	09/29/09	09/30/10	Utility	Tumbleweed software maintenance	Tumbleweed Communications Corp	Brand Name Competition
GS35F-0209S	02/28/11	03/04/11	Utility	Server software	EPM Solutions LLC	Brand Name Competition
HC1028-09-A-2006	01/06/11	02/05/11	Utility	Docking Laptops	Dell Federal Systems L P	Brand Name Competition
HC1028-09-A-2006	04/06/11	07/05/11	Utility	Dell Laptops and 19" LCD Monitors	Dell Federal Systems L P	Brand Name Competition
N00104-02-A-ZE82	12/07/10	12/06/11	Utility	Microsoft software for DECC	Insight Public Sector, Inc.	Brand Name Competition
N00104-02-A-ZE86	01/21/11	01/23/12	Utility	SQL Server software and licenses	Software House International Inc	Brand Name Competition
N00104-10-A-ZF30	03/23/11	04/22/11	Utility	SQL Server software and licenses	GovConnection Inc	Brand Name Competition
N00104-10-A-ZF30	04/14/11	05/14/11	Utility	SQL Server software and licenses	GovConnection Inc	Brand Name Competition
N00104-10-A-ZF30	04/14/11	05/14/11	Utility	SQL Server software and licenses	GovConnection Inc	Brand Name Competition
N00104-10-A-ZF30	07/01/11	07/30/11	Utility	SQL Server software and licenses	GovConnection Inc	Brand Name Competition
N00104-10-A-ZF30	07/15/11	08/14/11	Utility	SQL Server software and licenses	GovConnection Inc	Brand Name Competition
NNG07DA08B	08/23/11	11/21/11	Utility	Cisco Catalyst 4948 Switches and Maintenance Support	PC Mall Gov, Inc	Brand Name Competition
NNG07DA15B	08/04/11	09/03/12	Utility	Hardware	Dell Federal Systems L P	Brand Name Competition
NNG07DA15B	08/08/11	09/30/11	Utility	Riverbed & Steelhead Enterprise E-mail	Dell Federal Systems L P	Brand Name Competition
NNG07DA15B	08/26/11	09/25/11	Utility	Hardware and Support	Dell Federal Systems L P	Brand Name Competition
NNG07DA18B	08/13/11	11/30/11	Utility	DoD Enterprise Email SIPRNET Zeus Hardware and Support	Force 3 Inc	Brand Name Competition

Defense Information Systems Agency Contracts, Part 2

CONTRACT #	AWARD DATE	EXP DATE W/ OPT YRS	CATEGORY	DESCRIPTION	CONTRACTOR	COMPETITION TYPE TITLE
NNG07DA18B	08/13/11	11/30/11	Utility	DoD Enterprise Email SIPRNET Zeus HW and Maintenance	Force 3 Inc	Brand Name Competition
NNG07DA41B	04/08/11	08/09/11	Utility	Cisco Hardware and Maintenance Support	World Wide Technology, Inc	Brand Name Competition
NNG07DA41B	08/23/11	11/21/11	Utility	Cisco Hardware and Maintenance Support	World Wide Technology, Inc	Brand Name Competition
NNG07DA45B	08/04/11	09/30/11	Utility	Enterprise E-mail - Riverbed	ThunderCat Technology LLC	Brand Name Competition
NNG07DA45B	01/14/11	04/14/11	Utility	Enterprise E-mail - Riverbed	ThunderCat Technology LLC	Brand Name Competition
NNG07DA46B	08/03/11	09/02/12	Utility	Hardware & Maintenance	Alvarez & Associates LLC	Brand Name Competition
NNG07DA46B	08/03/11	09/02/12	Utility	Hardware & Maintenance	Alvarez & Associates LLC	Brand Name Competition
NNG07DA9B	12/01/10	11/30/11	Utility	Hardware & Maintenance	Unisys Corporation	Brand Name Competition
HC102808C2021	06/04/08	03/31/12	Professional	DISA Denver Facilities Engineering Support	S4 Inc	Full and Open
HC102808D2008	01/07/11	01/06/14	Professional	Edge Computing for Enterprise Services	Network Connectivity Solutions Corp	Full and Open
HC102808D2016	05/17/10	05/31/15	Professional	DISA-OKC Communications Network/Server Support	Caci Inc Federal	Full and Open
HC102808D2027	04/26/11	04/30/16	Professional	Enterprise Operations Technical and Application Support	Unisys Corporation	Full and Open
HC102808D2027	02/26/09	04/30/11	Professional	Enterprise Operations Technical and Application Support	Unisys Corporation	Full and Open
HC102808F2212	04/21/08	07/31/12	Professional	AKA - Access & Security Mgmt	ESCGov, Inc	Full and Open
HC102809F2878	09/29/09	09/30/14	Professional	Business Process Reengineering & Analysis	Lockheed Martin Management Systems Design	Full and Open
HC102810C2002	11/23/09	11/30/14	Professional	Windows/Linux/Unix System Admin Support	TecPort Solutions Inc	Other than Full and Open
HC102810F2187	03/24/10	03/23/14	Utility	Department of Defense (DoD) Identity Management Enterprise	Tangible Software Incorporated	Full and Open
HC102810F2627	09/10/10	08/15/11	Professional	Technical Support for Defense Enterprise Computing Centers	Northrop Grumman Systems Corporation	Full and Open
HC102810P2229	08/25/10	09/30/11	Utility	Server Support for Various DISA Sites	NexOne Inc	Other than Full and Open
HC102811C0102	12/01/10	02/28/15	Professional	Service Desk Agent Level 2 and 3 Augmentation.	NexOne Inc	Full and Open
HC102811C0123	08/15/11	08/15/16	Professional	Technical Support for DECCs	FoxHole Technology Inc	Full and Open
HC102811F0138	11/18/10	11/30/13	Professional	Defense Enterprise Computing Center - Oklahoma City	TechGuard Security LLC	Full and Open
HC102811F0725	09/15/11	12/19/11	Utility	DoD Enterprise Email SIPRNet	ThunderCat Technology LLC	Full and Open
HC102812C0006	12/13/11	12/14/16	Utility	Enterprise Email	NOVA Corporation	Other than Full and Open
HC102812F0088	12/16/11	12/14/12	Utility	Enterprise Email- RIM Elite Blackberry Enterprise Server	Blue Tech, Inc	Full and Open
N0010402AZE78	10/01/08	09/30/12	Utility	Microsoft Software	ASAP Software Express Inc	Full and Open
N0010410AZF30	06/16/11	07/16/11	Utility	Enterprise Email - Wave 7	GovConnection Inc	Full and Open
W91QUZ09D0038	05/24/11	05/24/12	Utility	Microsoft Premier Support Contract	Microsoft Corporation	Full and Open
W91QUZ09D0038	05/24/10	05/24/11	Utility	Microsoft Support	Microsoft Corporation	Full and Open



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON, DC 20310-0103

SAAL-SMC

FEB - 3 2012

MEMORANDUM FOR PROGRAM EXECUTIVE OFFICER, ENTERPRISE INFORMATION SYSTEMS

SUBJECT: Acquisition Decision Memorandum (ADM) for the Enterprise E-mail Program

1. References:

a. Section 353, National Defense Authorization Act (NDAA) FY2012, (Public Law 112-81), Designation and Limitation on Obligation and Expenditure of Funds for the Migration of Army Enterprise E-mail Services.

b. Memorandum, SAAL-SMC, January 25, 2012, subject: Acquisition Decision Memorandum (ADM) to initiate the Enterprise E-mail program.

2. The purpose of this ADM is to provide additional direction to the newly established Army Enterprise E-mail program.

3. After additional review of available documentation to include the Section 353 Report, I direct the following:

a. Army Enterprise E-mail has achieved Initial Operating Capability and is designated as a Services Category 2 acquisition, subject to annual review.

b. The Defense Information Systems Agency Enterprise E-mail Service solution is in the best technical and financial interests of the Army, and the acquisition of this solution was conducted in compliance with competition requirements.

Heidi Shyu

Heidi Shyu
Army Acquisition Executive

Attachment 4 – Acquisition Decision Memorandum, February 3, 2012

ACRONYM LIST

AAA	Army Audit Agency
AAE	Army Acquisition Executive
AD	Active Directory
AKO	Army Knowledge Online
AoA	Analysis of Alternatives
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
ASARC	Army Systems Acquisition Review Council
ASI	Authorized Service Interruption
BMCC	Brigade Migration Command Center
BSIT	Business Systems Information Technology
BSIT WG	Business Systems Information Technology Working Group
C2	Command and Control
CAC	Common Access Card
CBA	Cost-Benefit Analysis
CECOM	Communications-Electronics Command
CIO/G-6	Chief Information Officer/ G-6
CONUS	Contiguous United States
COOP	Continuity of Operations
DECC	DISA Enterprise Computing Center
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoDI	Department of Defense Instruction
DUSA-TEO	Deputy Under Secretary of the Army - Test and Evaluation Office
EASF	Enterprise Application and Services Forest
EDIPI	Electronic Data Interchange Personal Identifier
EDS-P	Enterprise Directory Services – Provisioning
EE	Enterprise E-mail
EGB	Enterprise Guidance Board
EIE	Enterprise Infrastructure Environment
EMMS	Enterprise Messaging as a Managed Service
EMSG	Email Security Gateway
HBSS	Host-Based Security System
HQDA	Headquarters, Department of the Army
IAVM	Information Assurance Vulnerability Management
IDS	Intrusion Detection Systems
IdSS	Identity Synchronization Service
IT	Information Technology
JCS	Java Communication Suite

MAC	Mission Assurance Category
MDA	Milestone Decision Authority
MDD	Materiel Development Decision
MSME	McAfee Security for Microsoft Exchange
NDAA	National Defense Authorization Act
NETCOM	Network Enterprise Technology Command
NIPRNET	Non-classified Internet Protocol Routing Network
NPEs	Non-Person Entities (mailboxes for other than people)
NSA	National Security Agency
OBT	Office of Business Transformation
OCONUS	Outside of Contiguous United States
OGC	Office of the General Counsel
OOB	Out-of-Band
PEO EIS	Program Executive Office Enterprise Information Systems
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PM	Project Manager
RFP	Request for Proposals
SAAT/PT	Security Architecture Analysis Team/Penetration Testing Team
SLA	Service Level Agreement
STIGs	Security Technical Implementation Guides
TRADOC	Training and Doctrine Command
TTPs	Tactics, Techniques and Procedures
USA/CMO	Under Secretary of the Army/Chief Management Officer
USCYBERCOM	United States Cyber Command
WCF	Web Content Filtering